IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF OKLAHOMA

JEFFREY LEWIN and AUDREY BERNSTEIN, individually and on behalf of all others similarly situated, Plaintiffs, v. SONIC CORP., Defendant.	Case No. ~~CIV-17-~~1047-F JURY TRIAL DEMANDED

PLAINTIFFS' CLASS ACTION COMPLAINT

Plaintiffs Jeffrey Lewin and Audrey Bernstein, (hereinafter, "Plaintiffs"), individually and on behalf of the Classes defined below, allege the following against Sonic Corp. ("Sonic") based upon personal knowledge with respect to themselves and on information and belief derived from, among other things, investigation of counsel and review of public documents as to all other matters:

NATURE OF THE CASE

1. Plaintiffs bring this class action case against Sonic for its failure to secure and safeguard consumers' personally identifiable information ("PII") which Sonic collected from various sources in connection with the operation of its restaurant business.

2. Sonic has acknowledged that a cybersecurity incident (the "Data Breach") occurred, resulting in the theft of its customers' PII, mainly consisting of credit card numbers and other information sufficient for wrongdoers to make fraudulent charges to Sonic customers' accounts.

3. The PII for Plaintiffs and the class of consumers they seek to represent was compromised due to Sonic's acts and omissions and their failure to properly protect the PII.

4. Sonic could have prevented this Data Breach. Data reaches at other restaurants, including one of its major competitors, Wendy's, have occurred.

5. Sonic disregarded the rights of Plaintiffs and Class members by intentionally, willfully, recklessly, or negligently failing to take adequate and reasonable measures to ensure its data systems were protected, failing to disclose to its customers the material fact that it did not have adequate computer systems and security practices to safeguard PII, failing to take available steps to prevent and stop the breach from ever happening, and failing to monitor and detect the breach on a timely basis.

6. As a result of the Data Breach, the PII of the Plaintiffs and Class members has been exposed to criminals for misuse. The injuries suffered by Plaintiffs and Class members, or likely to be suffered by Plaintiffs and Class members as a direct result of the Data Breach include:

a. unauthorized use of their PII;

b. theft of their personal and financial information;

c. costs associated with the detection and prevention of identity theft and unauthorized use of their financial accounts;

d. damages arising from the inability to use their PII;

e. loss of use of and access to their account funds and costs associated with inability to obtain money from their accounts or being limited in the amount of money they were permitted to obtain from their accounts, including missed payments on bills and loans, late charges and fees, and adverse effects on their credit including decreased credit scores and adverse credit notations;

f. costs associated with time spent and the loss of productivity or the enjoyment of one's life from taking time to address and attempt to ameliorate, mitigate and deal with the actual and future consequences of the Data Breach, including finding fraudulent charges, the costs of purchasing credit monitoring and identity theft protection services, and the stress, nuisance and annoyance of dealing with all issues resulting from the Data Breach;

g. the imminent and certainly impending injury flowing from potential fraud and identify theft posed by their PII being placed in the hands of

criminals and already misused via the sale of Plaintiffs and Class members' information on the Internet black market;

h. damages to and diminution in value of their PII entrusted to Sonic for the sole purpose of purchasing products and services from Sonic; and

i. the loss of Plaintiffs' and Class members' privacy.

7. The injuries to the Plaintiffs and Class members were directly and proximately caused by Sonic's failure to implement or maintain adequate data security measures for PII.

8. Further, Plaintiffs retain a significant interest in ensuring that their PII, which, while stolen, remains in the possession of Sonic, is protected from further breaches, and seeks to remedy the harms they have suffered on behalf of themselves and similarly situated consumers whose PII was stolen as a result of the Data Breach.

9. Plaintiffs bring this action to remedy these harms on behalf of themselves and all similarly situated individuals whose PII was accessed during the Data Breach. Plaintiffs seek the following remedies, among others: statutory damages under state and/or federal laws, reimbursement of out-of-pocket losses, other compensatory damages, further and more robust credit monitoring services with accompanying identity theft insurance, and injunctive relief including an order requiring Sonic to implement improved data security measures.

JURISDICTION AND VENUE

10. This Court has subject matter jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2). The amount in controversy exceeds $5 million exclusive of interest and costs. There are more than 100 putative class members. And, at least some members of the proposed Class have a different citizenship from Sonic.

11. This Court has personal jurisdiction over Sonic because it was founded in Oklahoma, maintains its headquarters and principal place of business in Oklahoma and regularly conducts business in Oklahoma, operating 276 of restaurants throughout the state.

12. Venue is proper in this Court pursuant to 28 U.S.C. § 1391(b) because Sonic's headquarters and principal place of business are in this District and a substantial part of the events, acts, and omissions giving rise to Plaintiffs' claims occurred in this District.

PARTIES

13. Plaintiff Jeffrey Lewin is a resident of Parkland, Florida. Plaintiff has been a customer at Sonic in the South Florida area and always pays with credit card. As a result of the Data Breach, Plaintiff Lewin has spent time and will continue to spend time monitoring his financial accounts for additional fraudulent activity.

14. Plaintiff Audrey Bernstein is a resident of Livingston, New Jersey. Plaintiff has been a customer at Sonic in New Jersey and always pays with credit card. As a result of the Data Breach, Plaintiff Bernstein has spent time and will continue to spend time monitoring her financial accounts for additional fraudulent activity.

15. Defendant Sonic Corp. is a Delaware Corp. with its headquarters and principal place of business located at 300 Johnny Bench Dr., Oklahoma City, OK 73104. Sonic may be served through its registered agent, Paige Bass, at its principal office address identified above.

STATEMENT OF FACTS

16. Sonic is the largest chain of drive-in restaurants in the United States. It operates over 3,500 restaurants in 44 states. Sonic accepts debit and credit card payments from its customers at each of its restaurants.

17. On September 26, 2017, Sonic announced that its payment system had been breached and up to five million credit card and debit card accounts had been stolen. This data is being sold on the blackmarket. Criminals use the data to make fraudulent charges to Sonic customers' accounts. *See* http://www.securityweek.com/breach-fast-food-chain-sonic-could-impact-millions-report.

18. There have been high profile data breaches of other restaurant chains, putting Sonic on notice of the need to be vigilant against and take steps to prevent data breaches. *See* https://www.qsrmagazine.com/restaurant-software/7-ways-protect-against-data-breach.

19. The payment system used by Sonic was more than thirty years old. While the company has been working to update its system, many restaurant locations have not yet been updated. *See* http://www.nrn.com/technology/sonic-team-helps-operators-reap-benefits-new-pos-system.

20. Additionally, Plaintiffs have suffered imminent and impending injury arising from the substantially increased risk of future fraud, identity theft and misuse posed by his PII being placed in the hands of criminals who have already, or will imminently, misuse such information.

21. Moreover, Plaintiffs have a continuing interest in ensuring that his private information, which remains in the possession of Sonic, is protected and safeguarded from future breaches.

22. At all relevant times, Sonic was well-aware, or reasonably should have been aware, that the PII collected, maintained and stored in the POS systems is highly sensitive, susceptible to attack, and could be used for wrongful purposes by third parties, such as identity theft and fraud.

23. It is well known and the subject of many media reports that PII is highly coveted and a frequent target of hackers. Despite the frequent public announcements of data breaches of other restaurants – Wendy's, Chipotle, etc. – Sonic continued to use an outdated, insufficient and inadequate system to protect the PII of Plaintiffs and Class members.

24. PII is a valuable commodity because it contains not only payment card numbers but PII as well. A "cyber blackmarket" exists in which criminals openly post stolen payment card numbers and other personal information on a number of underground Internet websites. PII is "as good as gold" to identity thieves because they can use victims' personal data to incur charges on existing accounts, or clone ATM, debit, or credit cards. Data from the Sonic breach have already appeared on such sites: http://www.securityweek.com/breach-fast-food-chain-sonic-could-impact-millions-report.

25. Legitimate organizations and the criminal underground alike recognize the value in PII contained in a merchant's data systems; otherwise, they would not aggressively seek or pay for it. For example, in "one of 2013's largest breaches . . . not only did hackers compromise the [card holder data] of three million customers, they also took registration data [containing PII] from 38 million users."[1]

[1] Verizon 2014 PCI Compliance Report, available at: http://www.cisco.com/c/dam/en_us/solutions/industries/docs/retail/verizon_pci2014.pdf (hereafter "2014 Verizon Report"), at 54 (last visited Sept. 8, 2017).

26. At all relevant times, Sonic knew, or reasonably should have known, of the importance of safeguarding PII and of the foreseeable consequences that would occur if its data security system was breached, including, specifically, the significant costs that would be imposed on individuals as a result of a breach.

27. Sonic was, or should have been, fully aware of the significant number of people whose PII it collected, and thus, the significant number of individuals who would be harmed by a breach of its payment system.

28. Unfortunately, and as alleged below, despite all of this publicly available knowledge of the continued compromises of PII in the hands of other third parties, Sonic's approach to maintaining the privacy and security of the PII of Plaintiffs and Class members was lackadaisical, cavalier, reckless, or at the very least, negligent.

29. The ramifications of Sonic's failure to keep Plaintiffs' and Class members' data secure are severe.

30. The FTC defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority."[2] The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person."[3]

---

[2] 17 C.F.R § 248.201 (2013).
[3] *Id.*

31. Personal identifying information is a valuable commodity to identity thieves once the information has been compromised. As the FTC recognizes, once identity thieves have personal information, "they can drain your bank account, run up your credit cards, open new utility accounts, or get medical treatment on your health insurance."[4]

32. Javelin Strategy and Research reports that identity thieves have stolen $112 billion in the past six years.[5]

33. Reimbursing a consumer for a financial loss due to fraud does not make that individual whole again. On the contrary, identity theft victims must spend numerous hours and their own money repairing the impact to their credit. After conducting a study, the Department of Justice's Bureau of Justice Statistics ("BJS") found that identity theft victims "reported spending an average of about 7 hours clearing up the issues" and resolving the consequences of fraud in 2014.[6]

34. There may be a time lag between when harm occurs versus when it is discovered, and also between when PII or PCD is stolen and when it is used.

---

[4] Federal Trade Commission, *Warning Signs of Identity Theft*, available at: https://www.consumer.ftc.gov/articles/0271-warning-signs-identity-theft (last visited April 10, 2017).

[5] *See* https://www.javelinstrategy.com/coverage-area/2016-identity-fraud-fraud-hits-inflection- point (last visited April 10, 2017).

[6] Victims of Identity Theft, 2014 (Sept. 2015) available at: http://www.bjs.gov/content/pub/pdf/vit14.pdf (last visited April 10, 2017).

According to the U.S. Government Accountability Office ("GAO"), which conducted a study regarding data breaches:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[7]

35. Plaintiffs and Class members now face years of constant surveillance of their financial and personal records, monitoring, and loss of rights. The Class is incurring and will continue to incur such damages in addition to any fraudulent use of their PII.

36. The PII of Plaintiffs and Class members is private and sensitive in nature and was left inadequately protected by Sonic.

37. The Data Breach was a direct and proximate result of Sonic's failure to properly safeguard and protect Plaintiffs' and Class members' PII from unauthorized access, use, and disclosure, as required by various state and federal regulations, industry practices, and the common law, including Sonic's failure to establish and implement appropriate administrative, technical, and physical safeguards to ensure

[7] GAO, Report to Congressional Requesters, at 29 (June 2007), available at http://www.gao.gov/new.items/d07737.pdf (last visited April 10, 2017).

the security and confidentiality of Plaintiffs' and Class members' PII to protect against reasonably foreseeable threats to the security or integrity of such information.

38. Sonic had the resources to prevent a breach, but neglected to timely and adequately invest in data security, despite the growing number of well-publicized data breaches.

39. Had Sonic remedied the deficiencies in its data security systems, followed security guidelines, and adopted security measures recommended by experts in the field, Sonic would have prevented the Data Breach and, ultimately, the theft of its customers' PII.

40. As a direct and proximate result of Sonic's wrongful actions and inaction and the resulting Data Breach, Plaintiffs and Class members have been placed at an imminent, immediate, and continuing increased risk of fraud, requiring them to take the time which they otherwise would have dedicated to other life demands such as work and effort to mitigate the actual and potential impact of the Data Breach on their lives including, inter alia, by placing "freezes" and "alerts" with credit reporting agencies, contacting their financial institutions, closing or modifying financial accounts, closely reviewing and monitoring their credit reports and accounts for unauthorized activity, and filing police reports. This time has been lost forever and cannot be recaptured. In all manners of life in this country, time has constantly been recognized as compensable, for many consumers it is the way they are compensated,

and even if retired from the work force, consumers should be free of having to deal with the consequences of a credit reporting agency's slippage, as is the case here.

41. Sonic's wrongful actions and inaction directly and proximately caused the theft and dissemination into the public domain of Plaintiffs' and Class members' PII, causing them to suffer, and continue to suffer, economic damages and other actual harm for which they are entitled to compensation, including:

a. theft of their personal and financial information;

b. unauthorized charges on their debit and credit card accounts;

c. the imminent and certainly impending injury flowing from potential fraud and identity theft posed by their PII being placed in the hands of criminals and already misused via the sale of Plaintiffs' and Class members' information on the black market;

d. the improper disclosure of their PII;

e. ascertainable losses in the form of out-of-pocket expenses and the value of their time reasonably incurred to remedy or mitigate the effects of the Data Breach;

f. ascertainable losses in the form of the loss of cash back or other benefits as a result of their inability to use certain accounts and cards affected by the Data Breach;

g. loss of use of and access to their account funds and costs associated with

the inability to obtain money from their accounts or being limited in the amount of money they were permitted to obtain from their accounts, including missed payments on bills and loans, late charges and fees, and adverse effects on their credit including adverse credit notations; and,

h. the loss of productivity and value of their time spent to address attempt to ameliorate, mitigate and deal with the actual and future consequences of the data breach, including finding fraudulent charges, cancelling and reissuing cards, purchasing credit monitoring and identity theft protection services, imposition of withdrawal and purchase limits on compromised accounts, and the stress, nuisance and annoyance of dealing with all such issues resulting from the Data Breach.

42. While the PII of Plaintiffs and members of the Class has been stolen, Sonic continues to hold PII of consumers, including Plaintiffs and Class members. Particularly because Sonic and has demonstrated an inability to prevent a breach or stop it from continuing even after being detected, Plaintiffs and members of the Class have an undeniable interest in insuring that their PII is secure, remains secure, is properly and promptly destroyed and is not subject to further theft.

CLASS ALLEGATIONS

43. Plaintiffs seek relief on behalf of themselves and as representatives of all others who are similarly situated. Pursuant to Fed. R. Civ. P. 23(a), (b)(2), (b)(3) and (c)(4), Plaintiffs seek certification of a Nationwide class defined as follows:

> All persons residing in the United States whose personally identifiable information was acquired by unauthorized persons in the data breach announced by Sonic in September 2017 (the "Nationwide Class").

44. Pursuant to Fed. R. Civ. P. 23, and in the alternative to claims asserted on behalf of the Nationwide Class, Plaintiffs assert claims under the laws of the individual States, and on behalf of separate statewide classes, defined as follows:

> All persons residing in Florida whose personally identifiable information was acquired by unauthorized persons in the data breach announced by Sonic in September 2017 (the "Statewide Classes").
>
> All persons residing in New Jersey whose personally identifiable information was acquired by unauthorized persons in the data breach announced by Sonic in September 2017 (the "Statewide Classes").

45. Excluded from each of the above Classes are any of Sonic's officers, directors and board members; all persons who make a timely election to be excluded from the Class; and the judges to whom this case is assigned and their immediate family.

46. Plaintiffs hereby reserve the right to amend or modify the class definition with greater specificity or division after having had an opportunity to conduct discovery.

47. Each of the proposed Classes meets the criteria for certification under Federal Rule of Civil Procedure 23(a), (b)(2), (b)(3) and (c)(4).

48. **Numerosity. Fed. R. Civ. P. 23(a)(1).** Consistent with Rule 23(a)(1), the members of the Class are so numerous and geographically dispersed that the joinder of all members is impractical. While the exact number of Class members is unknown to Plaintiffs at this time, the proposed Class include several million individuals whose PII was compromised in the Data Breach. Class members may be identified through objective means. Class members may be notified of the pendency of this action by recognized, Court-approved notice dissemination methods, which may include U.S. mail, electronic mail, internet postings, and/or published notice.

49. **Commonality. Fed. R. Civ. P. 23(a)(2) and (b)(3).** Consistent with Fed. R. Civ. P. 23(a)(2) and with 23(b)(3)'s predominance requirement, this action involves common questions of law and fact that predominate over any questions affecting individual Class members. The common questions include:

a. Whether Sonic had a duty to protect PII;

b. Whether Sonic knew or should have known of the susceptibility of their data security systems to a data breach;

c. Whether Sonic's security measures to protect their systems were reasonable in light of the measures recommended by data security experts;

d. Whether Sonic was negligent in failing to implement reasonable and adequate security procedures and practices;

e. Whether Sonic's failure to implement adequate data security measures allowed the breach to occur;

f. Whether Sonic's conduct constituted deceptive trade practices under state law;

g. Whether Sonic's conduct, including their failure to act, resulted in or was the proximate cause of the breach of its systems, resulting in the loss of the PII of Plaintiffs and Class members;

h. Whether Plaintiffs and Class members were injured and suffered damages or other acceptable losses because of Sonic's failure to reasonably protect its POS systems and data network; and,

i. Whether Plaintiffs and Class members are entitled to relief.

50. **Typicality**. **Fed. R. Civ. P. 23(a)(3).** Consistent with Fed. R. Civ. P. 23(a)(3), Plaintiffs' claims are typical of those of other Class members. Plaintiffs had their PII compromised in the Data Breach. Plaintiffs' damages and injuries are akin to other Class members and Plaintiffs seek relief consistent with the relief of the Class.

51. **Adequacy. Fed. R. Civ. P. 23(a)(4).** Consistent with Fed. R. Civ. P. 23(a)(4), Plaintiffs are adequate representatives of the Class because Plaintiffs are

members of the Class and are committed to pursuing this matter against Sonic to obtain relief for the Class. Plaintiffs have no conflict of interest with the Class. Plaintiffs' Counsel are competent and experienced in litigating class actions, including privacy litigation. Plaintiffs intend to vigorously prosecute this case and will fairly and adequately protect the Class' interests.

52. **Superiority. Fed. R. Civ. P. 23(b)(3).** Consistent with Fed. R. Civ. P23(b)(3), a class action is superior to any other available means for the fair and efficient adjudication of this controversy, and no unusual difficulties are likely to be encountered in the management of this class action. The quintessential purpose of the class action mechanism is to permit litigation against wrongdoers even when damages to individual plaintiffs may not be sufficient to justify individual litigation. Here, the damages suffered by Plaintiffs and the Class are relatively small compared to the burden and expense required to individually litigate their claims against Sonic, and thus, individual litigation to redress Sonic's wrongful conduct would be impracticable. Individual litigation by each Class member would also strain the court system. Individual litigation creates the potential for inconsistent or contradictory judgments, and increases the delay and expense to all parties and the court system. By contrast, the class action device presents far fewer management difficulties and provides the benefits of a single adjudication, economies of scale, and comprehensive supervision by a single court.

53. **Injunctive and Declaratory Relief.** Class certification is also appropriate under Fed. R. Civ. P. 23(b)(2) and (c). Defendant, through its uniform conduct, has acted or refused to act on grounds generally applicable to the Class as a whole, making injunctive and declaratory relief appropriate to the Class as a whole.

54. Likewise, particular issues under Rule 23(c)(4) are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Such particular issues include, but are not limited to:

a. Whether Sonic owed a legal duty to Plaintiffs and the Class to exercise due care in collecting, storing, and safeguarding their PII;

b. Whether Sonic's security measures were reasonable in light of data security recommendations, and other measures recommended by data security experts;

c. Whether Sonic failed to adequately comply with industry standards amounting to negligence;

d. Whether Sonic failed to take commercially reasonable steps to safeguard the PII of Plaintiffs and the Class members; and,

e. Whether adherence to data security recommendations, and measures recommended by data security experts would have

reasonably prevented the Data Breach.

55. Finally, all members of the proposed Classes are readily ascertainable. Sonic has access to information regarding the Data Breach, the time period of the Data Breach, and which individuals were potentially affected. Using this information, the members of the Class can be identified and their contact information ascertained for purposes of providing notice to the Class.

COUNT I
NEGLIGENCE

(ON BEHALF OF PLAINTIFFS AND THE NATIONWIDE CLASS, OR, ALTERNATIVELY, PLAINTIFFS AND THE SEPARATE STATEWIDE CLASSES)

56. Plaintiffs restate and re-allege Paragraphs 1 through 55 as if fully set forth herein.

57. Upon accepting and storing the PII of Plaintiffs and Class Members in its computer systems and on its networks, Sonic undertook and owed a duty to Plaintiffs and Class Members to exercise reasonable care to secure and safeguard that information and to use commercially reasonable methods to do so. Sonic knew that the PII was private and confidential and should be protected as private and confidential.

58. Sonic owed a duty of care not to subject Plaintiffs, along with their PII, and Class members to an unreasonable risk of harm because they were foreseeable and probable victims of any inadequate security practices.

59. Sonic owed numerous duties to Plaintiffs and to members of the Nationwide Class, including the following:

a. to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting and protecting PII in its possession;

b. to protect PII using reasonable and adequate security procedures and systems that are compliant with industry-standard practices; and

c. to implement processes to quickly detect a data breach and to timely act on warnings about data breaches.

60. Sonic also breached its duty to Plaintiffs and the Class Members to adequately protect and safeguard PII by knowingly disregarding standard information security principles, despite obvious risks. Further, Sonic failed to provide adequate supervision and oversight of the PII with which they were and are entrusted, in spite of the known risk and foreseeable likelihood of breach and misuse, which permitted an unknown third party to gather PII of Plaintiffs and Class Members, misuse the PII and intentionally disclose it to others without consent.

61. Sonic knew, or should have known, of the risks inherent in collecting and storing PII, the vulnerabilities of its data security systems, and the importance of

adequate security. Sonic knew about numerous, well-publicized data breaches, including the breaches at Wendy's, Chipotle, etc.

62. Sonic knew, or should have known, that their data systems and networks did not adequately safeguard Plaintiffs' and Class Members' PII.

63. Sonic breached its duties to Plaintiffs and Class Members by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard PII of Plaintiffs and Class Members.

64. Because Sonic knew that a breach of its systems would damage millions of individuals, including Plaintiffs and Class members, Sonic had a duty to adequately protect their data systems and the PII contained thereon.

65. Sonic's own conduct also created a foreseeable risk of harm to Plaintiffs and Class members and their PII. Sonic's misconduct included failing to: (1) secure its systems, despite knowing their vulnerabilities, (2) comply with industry standard security practices, (3) implement adequate system and event monitoring, and (4) implement the systems, policies, and procedures necessary to prevent this type of data breach.

66. Sonic also had independent duties under state and/or federal laws that required it to safeguard Plaintiffs' and Class members' PII.

67. Sonic breached its duties to Plaintiffs and Class members in numerous ways, including:

a. by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard PII of Plaintiffs and Class members;

b. by creating a foreseeable risk of harm through the misconduct previously described;

c. by failing to implement adequate security systems, protocols and practices sufficient to protect Plaintiffs' and Class members' PII both before and after learning of the Data Breach; and

d. by failing to comply with the minimum industry data security standards during the period of the Data Breach.

68. Through Sonic's acts and omissions described in this Complaint, including Sonic's failure to provide adequate security and its failure to protect PII of Plaintiffs and Class members from being foreseeably captured, accessed, disseminated, stolen and misused, Sonic unlawfully breached its duty to use reasonable care to adequately protect and secure PII of Plaintiffs and Class members during the time it was within its possession or control.

69. Upon information and belief, Sonic improperly and inadequately safeguarded PII of Plaintiffs and Class Members in deviation of standard industry rules, regulations, and practices at the time of the unauthorized access. Sonic's failure to take proper security measures to protect sensitive PII of Plaintiffs and Class

members as described in this Complaint, created conditions conducive to a foreseeable, intentional criminal act, namely the unauthorized access of PII of Plaintiffs and Class members.

70. Sonic's conduct was grossly negligent and departed from all reasonable standards of care, including, but not limited to: failing to adequately protect the PII; failing to conduct regular security audits; failing to provide adequate and appropriate supervision of persons having access to PII of Plaintiffs and Class members; and failing to provide Plaintiffs and Class members with timely and sufficient notice that their sensitive PII had been compromised.

71. Neither Plaintiffs nor the other Class members contributed to the Data Breach and subsequent misuse of their PII as described in this Complaint.

72. As a direct and proximate cause of Sonic's conduct, Plaintiffs and the Class suffered damages including, but not limited to: damages arising from the unauthorized charges on their debit or credit cards or on cards that were fraudulently obtained through the use of the PII of Plaintiffs and Class Members; damages arising from their inability to use their debit or credit cards because those cards were cancelled, suspended, or otherwise rendered unusable as a result of the Data Breach and/or false or fraudulent charges stemming from the Data Breach, including but not limited to late fees charges and foregone cash back rewards; damages from lost time and effort to mitigate the actual and potential impact of the Data Breach on their lives

including, inter alia, by placing "freezes" and "alerts" with credit reporting agencies, contacting their financial institutions, closing or modifying financial accounts, closely reviewing and monitoring their credit reports and accounts for unauthorized activity, and filing police reports and damages from identity theft, which may take months if not years to discover and detect, given the far-reaching, adverse and detrimental consequences of identity theft and loss of privacy. The nature of other forms of economic damage and injury may take years to detect, and the potential scope can only be assessed after a thorough investigation of the facts and events surrounding the theft mentioned above.

COUNT II
NEGLIGENCE PER SE

(ON BEHALF OF PLAINTIFFS AND THE NATIONWIDE CLASS, OR, ALTERNATIVELY, PLAINTIFFS AND THE SEPARATE STATEWIDE CLASSES)

73. Plaintiffs restate and reallege Paragraphs 1 through 72 as if fully set forth herein.

74. Section 5 of the FTC Act prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Sonic, of failing to use reasonable measures to protect PII. The FTC publications and orders described above also form part of the basis of Sonic's duty in this regard.

75. Sonic violated Section 5 of the FTC Act by failing to use reasonable measures to protect PII and not complying with applicable industry standards, as described in detail herein.

76. Sonic's violation of Section 5 of the FTC Act constitutes negligence *per se*.

77. Plaintiffs and Class Members are within the class of persons that the FTC Act was intended to protect.

78. The harm that occurred as a result of the Data Breach is the type of harm the FTC Act was intended to guard against. The FTC has pursued enforcement actions against businesses, which, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiffs and the Class.

79. As a direct and proximate result of Sonic's negligence *per se*, Plaintiffs and the Class have suffered, and continue to suffer, injuries damages arising from their inability to use their debit or credit cards because those cards were cancelled, suspended, or otherwise rendered unusable as a result of the Data Breach and/or false or fraudulent charges stemming from the Data Breach, including but not limited to late fees charges and foregone cash back rewards; damages from lost time and effort to mitigate the actual and potential impact of the Data Breach on their lives including, inter alia, by placing "freezes" and "alerts" with credit reporting agencies, contacting

their financial institutions, closing or modifying financial accounts, closely reviewing and monitoring their credit reports and accounts for unauthorized activity, and filing police reports and damages from identity theft, which may take months if not years to discover and detect, given the far-reaching, adverse and detrimental consequences of identity theft and loss of privacy.

COUNT III
DECLARATORY JUDGMENT

(ON BEHALF OF PLAINTIFFS AND THE NATIONWIDE CLASS, OR, ALTERNATIVELY, PLAINTIFFS AND THE SEPARATE STATEWIDE CLASSES)

80. Plaintiffs restate and reallege Paragraphs 1 through 79 as if fully set forth herein.

81. As previously alleged, Plaintiffs and Class members entered into an implied contract that required Sonic to provide adequate security for the PII it collected from their payment card transactions. As previously alleged, Sonic owes duties of care to Plaintiffs and Class members that require it to adequately secure PII.

82. Sonic still possesses PII pertaining to Plaintiffs and Class members.

83. Sonic has made no announcement or notification that it has remedied the vulnerabilities in its computer data systems, and, most importantly, its systems.

84. Accordingly, Sonic has not satisfied its contractual obligations and legal duties to Plaintiffs and Class members. In fact, now that Sonic's lax approach towards

data security has become public, the PII in its possession is more vulnerable than previously.

85. Actual harm has arisen in the wake of the Sonic Data Breach regarding Sonic's contractual obligations and duties of care to provide data security measures to Plaintiffs and Class members.

86. Plaintiffs, therefore, seeks a declaration that (a) Sonic's existing data security measures do not comply with its contractual obligations and duties of care, and (b) in order to comply with its contractual obligations and duties of care, Sonic must implement and maintain reasonable security measures, including, but not limited to:

a. engaging third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Sonic's systems on a periodic basis, and ordering Sonic to promptly correct any problems or issues detected by such third-party security auditors;

b. engaging third-party security auditors and internal personnel to run automated security monitoring;

c. auditing, testing, and training its security personnel regarding any new or modified procedures;

d. segmenting PII by, among other things, creating firewalls and access

controls so that if one area of Sonic is compromised, hackers cannot gain access to other portions of Sonic systems;

e. purging, deleting, and destroying in a reasonable secure manner PII not necessary for its provisions of services;

f. conducting regular database scanning and securing checks;

g. routinely and continually conducting internal training and education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach; and

h. educating its customers about the threats they face as a result of the loss of their financial and personal information to third parties, as well as the steps Sonic customers must take to protect themselves.

COUNT IV

VIOLATION OF FLORIDA'S UNFAIR TRADE PRACTICES ACT, FLA. STAT. § 501.201, *ET SEQ*.

(ON BEHALF OF PLAINTIFF LEWIN AND THE SEPARATE STATEWIDE CLASSES)

87. Plaintiff Lewin restates and realleges Paragraphs 1 through 86 as if fully set forth herein.

88. At all relevant times, Florida Subclass members were "consumers" within the meaning of FDUPTA.

89. Sonic is engaged in trade and commerce in Florida.

90. Plaintiff and Class members entrusted Sonic with their PII.

91. As alleged herein this Complaint, Sonic engaged in unfair or deceptive acts or practices in the conduct of consumer transactions, including the following, in violation of the FDUTPA:

a. failure to maintain the security of credit and/or debit card account information;

b. failure to maintain adequate computer systems and data security practices to safeguard credit and debit card information and other PII;

b. failure to disclose that its computer systems and data security practices were inadequate to safeguard credit and debit card information and other PII from theft;

d. continued acceptance of PII and storage of other personal information after Sonic knew or should have known of the security vulnerabilities of the systems that were exploited in the Data Breach;

e allowing unauthorized persons to have access to and make unauthorized charges to its customers' credit and/or debit card accounts.

92. Sonic knew or should have known that its computer systems and data security practices were inadequate to safeguard the PII of Plaintiff and Class

members, deter hackers, and detect a breach within a reasonable time, and that the risk of a data breach was highly likely.

93. As a direct and proximate result of Sonic's violation of the FDUTPA, Plaintiff Lewin and Class members suffered damages including, but not limited to: damages arising from the unauthorized charges on their debit or credit cards or on cards that were fraudulently obtained through the use of the PII of Plaintiff and Class Members; damages arising from their inability to use their debit or credit cards or accounts because those cards or accounts were cancelled, suspended, or otherwise rendered unusable as a result of the Data Breach and/or false or fraudulent charges stemming from the Data Breach, including but not limited to late fees charges and foregone cash back rewards; damages from lost time and effort to mitigate the actual and potential impact of the Data Breach on their lives including, *inter alia*, by placing "freezes" and "alerts" with credit reporting agencies, contacting their financial institutions, closing or modifying financial accounts, closely reviewing and monitoring their credit reports and accounts for unauthorized activity, and filing police reports and damages from identity theft, which may take months if not years to discover and detect, given the far-reaching, adverse and detrimental consequences of identity theft and loss of privacy. The nature of other forms of economic damage and injury may take years to detect, and the potential scope can only be assessed after

a thorough investigation of the facts and events surrounding the theft mentioned above.

94. Also as a direct result of Sonic's knowing violation of the FDUTPA, Plaintiff Lewin and Class members are entitled to damages as well as injunctive relief, including, but not limited to:

a. Ordering that Sonic engage third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Sonic's systems on a periodic basis, and ordering Sonic to promptly correct any problems or issues detected by such third-party security auditors;

b. Ordering that Sonic engage third-party security auditors and internal personnel to run automated security monitoring;

c. Ordering that Sonic audit, test, and train its security personnel regarding any new or modified procedures;

d. Ordering that Sonic segment PII by, among other things, creating firewalls and access controls so that if one area of Sonic is compromised, hackers cannot gain access to other portions of Sonic systems;

e. Ordering that Sonic purge, delete, and destroy in a reasonable secure manner PII not necessary for its provisions of services;

f. Ordering that Sonic conduct regular database scanning and securing checks;

g. Ordering that Sonic routinely and continually conduct internal training and education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach; and

h. Ordering Sonic to meaningfully educate its customers about the threats they face as a result of the loss of their financial and personal information to third parties, as well as the steps Sonic customers must take to protect themselves.

95. Plaintiff brings this action on behalf of himself and Class Members for the relief requested above and for the public benefit in order to promote the public interests in the provision of truthful, fair information to allow consumers to make informed purchasing decisions and to protect Plaintiff and Class members and the public from Sonic's unfair methods of competition and unfair, deceptive, fraudulent, unconscionable and unlawful practices. Sonic's wrongful conduct as alleged in this Complaint has had widespread impact on the public at large.

96. Plaintiff Lewin and the Florida Subclass seek actual damages under Fla. Stat. § 501.211 (2) and all fees, costs, and expenses allowed by law, including attorney's fees and costs, pursuant to Federal Rule of Civil Procedure 23 and Fla. Stat. §§ 501.2105 and 501.211, to be proven at trial.

COUNT V

VIOLATION OF NEW JERSEY'S CONSUMER FRAUD ACT, N.J. STAT. ANN. § 56:8-1, *ET SEQ*.

(ON BEHALF OF PLAINTIFF BERNSTEIN AND THE SEPARATE STATEWIDE CLASSES)

97. Plaintiff Bernstein restates and realleges Paragraphs 1 through 96 as if fully set forth herein.

98. As alleged herein this Complaint, Sonic, while operating in New Jersey, engaged in unconscionable commercial practices, deception, misrepresentation, and the knowing concealment, suppression, and omission of material facts with intent that others rely on such concealment, suppression, and omission, in connection with the sale and advertisement of services, in violation of N.J. Stat. Ann. § 56.8-2. This includes, but is not limited to the following:

c. failure to maintain the security of credit and/or debit card account information;

d. failure to maintain adequate computer systems and data security practices to safeguard credit and debit card information and other PII;

b. failure to disclose that its computer systems and data security practices were inadequate to safeguard credit and debit card information and other PII from theft;

d. continued acceptance of PII and storage of other personal information

after Sonic knew or should have known of the security vulnerabilities of the systems that were exploited in the Data Breach;

e allowing unauthorized persons to have access to and make unauthorized charges to its customers' credit and/or debit card accounts.

99. Sonic knew or should have known that its computer systems and data security practices were inadequate to safeguard the PII of Plaintiff Bernstein and Class members, deter hackers, and detect a breach within a reasonable time, and that the risk of a data breach was highly likely.

100. As a direct and proximate result of Sonic's violation of the New Jersey Consumer Fraud Act, Plaintiff and Class members suffered damages including, but not limited to: damages arising from the unauthorized charges on their debit or credit cards or on cards that were fraudulently obtained through the use of the PII of Plaintiff and Class Members; damages arising from their inability to use their debit or credit cards or accounts because those cards or accounts were cancelled, suspended, or otherwise rendered unusable as a result of the Data Breach and/or false or fraudulent charges stemming from the Data Breach, including but not limited to late fees charges and foregone cash back rewards; damages from lost time and effort to mitigate the actual and potential impact of the Data Breach on their lives including, *inter alia*, by placing "freezes" and "alerts" with credit reporting agencies, contacting their

financial institutions, closing or modifying financial accounts, closely reviewing and monitoring their credit reports and accounts for unauthorized activity, and filing police reports and damages from identity theft, which may take months if not years to discover and detect, given the far-reaching, adverse and detrimental consequences of identity theft and loss of privacy. The nature of other forms of economic damage and injury may take years to detect, and the potential scope can only be assessed after a thorough investigation of the facts and events surrounding the theft mentioned above.

101. Also as a direct result of Sonic's knowing violation of the New Jersey Consumer Fraud Act, Plaintiff Bernstein and Class members are entitled to damages as well as injunctive relief, including, but not limited to:

a. Ordering that Sonic engage third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Sonic's systems on a periodic basis, and ordering Sonic to promptly correct any problems or issues detected by such third-party security auditors;

b. Ordering that Sonic engage third-party security auditors and internal personnel to run automated security monitoring;

c. Ordering that Sonic audit, test, and train its security personnel regarding any new or modified procedures;

d. Ordering that Sonic segment PII by, among other things, creating firewalls and access controls so that if one area of Sonic is compromised, hackers cannot gain access to other portions of Sonic systems;

e. Ordering that Sonic purge, delete, and destroy in a reasonable secure manner PII not necessary for its provisions of services;

f. Ordering that Sonic conduct regular database scanning and securing checks;

g. Ordering that Sonic routinely and continually conduct internal training and education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach; and

h. Ordering Sonic to meaningfully educate its customers about the threats they face as a result of the loss of their financial and personal information to third parties, as well as the steps Sonic customers must take to protect themselves.

102. Plaintiff brings this action on behalf of herself and Class Members for the relief requested above and for the public benefit in order to promote the public interests in the provision of truthful, fair information to allow consumers to make informed purchasing decisions and to protect Plaintiff and Class members and the public from Sonic's unfair methods of competition and unfair, deceptive, fraudulent,

unconscionable and unlawful practices. Sonic's wrongful conduct as alleged in this Complaint has had widespread impact on the public at large.

103. Plaintiff and the New Jersey Subclass also seeks actual damages, injunctive and/or other equitable relief and treble damages, and attorney's fees and costs pursuant to Federal Rule of Civil Procedure 23 and N.J. Stat. Ann. § 56:8-19.

COUNT VI

VIOLATION OF THE NEW JERSEY DATA BREACH ACT

(ON BEHALF OF PLAINTIFF BERNSTEIN AND THE SEPARATE STATEWIDE CLASSES

104. Plaintiff Bernstein restates and realleges Paragraphs 1 through 103 as if fully set forth herein. Plaintiff and the other members of the New Jersey Sub-Class are consumers who provided PII to Sonic by making purchases through her credit card for personal and private use.

105. By failing to timely notify Sonic customers of the Data Breach, Sonic violated N.J. Stat. Ann. §56:8-163(a), et seq., which provides:

> (a) Any business that conducts business in New Jersey, or any public entity that compiles or maintains computerized records that include personal information, shall disclose any breach of security of those computerized records following discovery or notification of the breach to any customer who is a resident of New Jersey whose personal information was, or is reasonably believed to have been, accessed by an unauthorized person. The disclosure to a customer shall be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement, as provided in subsection c. of this section, or any measures necessary to determine the scope of the breach and restore the reasonable integrity of the data system. Disclosure of a breach of security to a customer

> shall not be required under this section if the business or public entity establishes that misuse of the information is not reasonably possible. Any determination shall be documented in writing and retained for five years.
>
> * * *
>
> (c)(2) The notification required by this section shall be delayed if a law enforcement agency determines that the notification will impede a criminal or civil investigation and that agency has made a request that the notification be delayed. The notification required by this section shall be made after the law enforcement agency determines that its disclosure will not compromise the investigation and notifies that business or public entity.
>
> * * *
>
> 56:8-166 It shall be an unlawful practice and a violation of P.L. 1960, c.39 (C.56:8-1 et seq.) to willfully, knowingly or recklessly violate sections 10 through 13 of this amendatory and supplementary act.

106. The Sonic Data Breach constituted a breach of the Sonic security system within the meaning of the above New Jersey data breach statute and the data breached was protected and covered by the data breach statute.

107. Sonic unreasonably delayed informing the public, including Plaintiff and the members of the Class, about the Data Breach after Sonic knew or should have known that the Data Breach had occurred.

108. While the Data Breach and stealing of customer's personal information was known or should have been known to Sonic, Sonic did not notify customers of the data breach until September 26, 2017.

109. Thus, Sonic failed to disclose the Data Breach to Plaintiff and the other members of the Class without unreasonable delay and in the most expedient time possible.

110. Sonic has provided no indication that any law enforcement agency requested that Sonic delay notification. Plaintiff and the other members of the Sub-Class suffered harm directly resulting from Sonic's failure to provide and the delay in providing notification of the data breach with timely and accurate notice as required by law.

111. As a result of said practices, Sonic has directly, foreseeably, and proximately caused damages to Plaintiff Bernstein and the other members of the Class. Had Sonic provided timely and accurate notice of the Data Breach Plaintiff Bersntein and the other members of the Class would have been able to avoid and/or attempt to ameliorate or mitigate the damages and harm resulting in the unreasonable delay by Sonic in providing notice. Plaintiff and the Class members could have avoided providing further data to Sonic could have avoided use of Sonic's services, and otherwise have tried to avoid the harm caused by Sonic's delay in providing timely and accurate notice.

REQUEST FOR RELIEF

WHEREFORE, Plaintiffs, individually and on behalf of all Class members proposed in this Complaint, respectfully requests that the Court enter judgment in

their favor and against Sonic as follows:

a. For an Order certifying the Classes, as defined herein, and appointing Plaintiffs and their Counsel to represent the Nationwide Class, or in the alternative the separate Statewide Classes;

b. For equitable relief enjoining Sonic from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of Plaintiffs' and Class members' PII, and from refusing to issue prompt, complete and accurate disclosures to the Plaintiffs and Class members;

c. For equitable relief compelling Sonic to use appropriate cyber security methods and policies with respect to consumer data collection, storage and protection and to disclose with specificity to class members the type of PII compromised;

d. For an award of damages, as allowed by law in an amount to be determined;

e. For an award of attorneys' fees costs and litigation expenses, as allowable by law;

f. For prejudgment interest on all amounts awarded; and

g. Such other and further relief as this court may deem just and proper.

JURY TRIAL DEMAND

Plaintiffs demand a jury trial on all issues so triable. Dated: October 2, 2017

Respectfully Submitted,

s/ William B. Federman
William B. Federman, OBA #2853
Carin L. Marcussen, OBA #19869
Joshua D. Wells, OBA # 22334
FEDERMAN & SHERWOOD
10205 North Pennsylvania Ave.
Oklahoma City, OK 73120
Telephone: (405) 235-1560
Facsimile: (405) 239-2112
Email: wbf@federmanlaw.com
clm@federmanlaw.com
jdw@federmanlaw.com

Melissa R. Emert. Esq.
(to be admitted pro hac vice)
Howard T. Longman, Esq.
(to be admitted pro hac vice)
STULL, STULL & BRODY
6 East 45th Street
New York, NY 10017
Telephone: (212) 687-7230
Facsimile: (212) 490-2022
Email: memert@ssbny.com
hlongman@ssbny.com

Attorneys for Plaintiffs
and the Proposed Classes